○ SUMMER 05 | ○ TENTH EDITION

PDSD news

UNITED STATES DEPARTMENT OF AGRICULTURE
PERSONNEL & DOCUMENT SECURITY DIVISION (PDSD)
USDA/DA/OPPM/PDSD
202/720-7373

Helping you achieve your e-QIP goals

The Personnel and Document Security Division (PDSD) saw a significant improvement in e-QIP submissions by individual agencies during the last quarter. Specifically, the Animal and Plant Health Inspection Service, Farm Services Agency, Forest Service, National Finance Center, and Food Safety Inspection Service each successfully submitted forms using the new electronic system. To date, four USDA agencies have met or exceeded the goal of submitting 75% of their national security forms to the Office of Personnel Management (OPM) by the end of the third quarter of fiscal year 2005. Congratulations to the Agricultural Research Service, Foreign Agricultural Service, Office of the Chief Information Officer, and the Office of the Inspector General for rising to the challenge!

Overall, e-QIP submissions are still lower than expected, as only 34% of the total requests for national security clearances were submitted through e-QIP during the third quarter. In an effort to boost usage in the remaining agencies/staff offices by the end of the fiscal year, the PDSD sponsored refresher e-QIP training sessions at the Office of Personnel Management (OPM) on July 7th and July 19th.

As a reminder, the PDSD will no longer accept paper submissions of the Standard Form 86 after September 9, 2005 (reference Personnel Security Bulletin # 05-03, located at: http://www.usda.gov/da/pdsd/bulletin05-03.pdf). Furthermore, as soon as the OPM releases the Standard Form 85-P, "Questionnaire for Public Trust Positions," for use in USDA, the PDSD will stop accepting paper submissions without a written waiver.

BULLETIN WATCH

The Personnel Security Branch issued two new Bulletins on July 7, 2005. **Personnel Security Bulletin #05-02, "30-day Suspense for Accomplishing Initial and Refresher Security Briefings,"** establishes new suspense dates by which security indoctrinations and refresher briefings must be accomplished. **Personnel Security Bulletin #05-03, "End of Year Case Processing – Action Due Prior to September 9, 2005,"** sets the cut-off deadline for all FY-05 background investigation requests to ensure timely processing to OPM. To view these Bulletins, visit our website at http://www.usda.gov/da/pdsd/bulletins.htm.

The State of Background Investigations

OPM delivers testimony on the federal government's background investigations process to Senate subcommittee.

OPM Deputy Associate Director, Kathy Dillaman, testified before the Senate Subcommittee on Oversight of Government Management on June 29, 2005, on efforts to expedite and consolidate elements of the personnel security investigations program that support issuing security clearances.

According to Dillaman, OPM expects to receive over 1.4 million new requests for various levels of background investigations from over 100 federal agencies this fiscal year. Over 550,000 of those will be to support security clearance actions.

Dillaman reiterated how the federal investigations process is being upgraded. "Under the terms of the Intelligence Reform and Terrorism Prevention Act of 2004, OPM is required to establish, operate, and maintain an intergrated, secure, consolidated database of security clearances with information on granting, denial, or revocation of clearance actions pertaining to military, civilian, or government contractor personnel," said Dillaman.

"OPM's Clearance Verification System (CVS) was built on a flexible platform with ample capacity to expand the content of these records and provide access for authorized users. We are meeting with the clearance granting agencies now to determine what additional data elements are needed as well as the most effective methods for recording these actions and keeping the data accurate and up to date, " said Dillaman.

Dillaman also discussed the Electronic Questionnaires for Investigations Processing (e-QIP) stating that 27 agencies use the system and over 17,000 investigations have been requested electronically.

Executive Order 13381

Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information.

President Bush issued Executive Order 13381 on June 27, 2005, to implement security clearance reform. The policy under this order states, "To the extent consistent with safeguarding the security of the United States and protecting classified national security information from unauthorized disclosure, agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal."

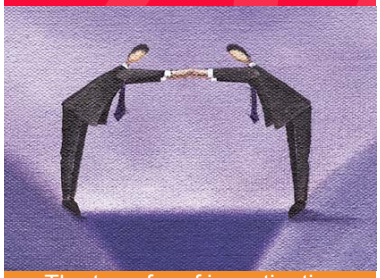
The House Government Reform Committee and the Government Accountability Office (GAO) had pushed for the executive order. "The signing of Executive Order 13381 is a major step forward on the road to meaningful security clearance process reform," said Committee Chairman Tom Davis, R-VA. "Large backlogs, long wait times and convoluted bureaucratic hierarchies have plagued this process for years, endangering national security and costing the taxpayers millions of dollars a year."

GAO report, *"DOD Personnel Clearances: Some Progress Has Been Made, but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation"* (http://www.gao.gov/new.items/d05842t.pdf), shared its findings on security clearance backlogs with the Senate in June. A primary objective of this executive order is to fix one of the problems the GAO report pointed out by requiring agencies to accept clearances granted by others agencies. The Office of Management and Budget will now oversee agency reciprocation.

Exective Order 13381: http://www.whitehouse.gov/news/releases/2005/06/20050628-4.html

GROWING PAINS:

OPM and DoD struggle on merger



The transfer of investigative functions from the Defense Department to the Office of Personnel Management is hindering, not helping the process so far, according to the Government Accountability Office.

Derek Stewart, the Director of Defense Capabilities and Management at GAO, testified that "despite having two years…DoD and OPM did not ensure that software was available for the seamless submission of requests from DoD's system to OPM's." DoD cannot make full use of OPM's e-QIP system. DoD is now developing software that will convert the department's submissions into the e-QIP format.

OPM has had a problem with the turnover rate in the ranks of investigators, most of whom are contract employees. Auditors concluded that OPM would need to add about 3,800 full-time investigators in order to clear the backlog of more than 185,000. This high turnover rate could leave OPM with a large number of investigative staff with limited experience. OPM stated the quality of the investigations is not where they would like it to be. OPM's current goals for completing a case allows for more time than did the DoD goals.

Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers

Research conducted by the Defense Personnel Security Research Center (PERSEREC)
May 2005

PERSEREC recently conducted a study of supervisor and coworker reporting of security-related information. Explanations were offered by security managers and by focus group participants as to why many security-related behaviors are under reported. The main problem is that people are hesitant to report suitability behaviors, such as excessive use of alcohol, because they are not able to see a direct link between the particular human problem and national security. Consequently, PERSEREC developed a clear, succinct list of behaviors titled *CORE*, *Counterintelligence Reporting Essentials*, that could pose a potential threat to national security and thus should be reported if observed. Members of various counterintelligence agences in the government reviewed and edited the list. It has since been included in the new DoD Instruction 5240.6 *Counterintelligence Awareness, Briefing, and Reporting Programs*. PERSEREC has also developed a brochure based on these items as an educational tool to help departments that have need of security education materials. The behaviors fall under the headings, *Recruitment, Information Collection, Information Transmittal, and Suspicious Behaviors*.

Supervisors and coworkers are the first line of defense against espionage. The government relies on individuals to protect national security by reporting any behavior that is observed that may be related to a potential compromise of classified information. Presented below is a focused list of serious counterintelligence and security-related behaviors that, if observed or learned about, should be reported immediately to appropriate security authorities. The list of behaviors is not intended to be exhaustive. You should report any additional behaviors that may parallel or exceed the concerns listed. The entire report can be viewed at http://www.fas.org/sgp/othergov/dod/cireporting.pdf.

RECRUITMENT
Reportable Behaviors

- You become aware of a colleague having contact with an individual who is known to be, or is suspected of being, associated with a foreign intelligence, security, or terrorist organization.
- You discover that a colleague has not reported an offer of financial assistance by a foreign national other than close family.
- You find out that a colleague has failed to report a request for classified or unclassified information outside official channels by a foreign national or anyone without authorization or need-to-know.
- You become aware of a colleague engaging in illegal activity or if a colleague asks you to engage in any illegal activity.

INFORMATION COLLECTION
Reportable Behaviors

- A colleague asks you to obtain classified or other protected information in any format to which the person does not have authorized access.
- A colleague asks you to witness signatures for destruction of classified information when you did not observe the destruction.
- You observe a colleague operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed.
- You become aware of the existence of any listening or surveillance devices in sensitive or secure areas.
- You find out a colleague has been keeping classified material at home or any other unauthorized place.
- You discover a colleague acquiring access to classified or unclassified automated information systems without authorization.
- You observe a colleague seeking to obtain access to sensitive information inconsistent with present duty requirements.

INFORMATION TRANSMITTAL
Reportable Behaviors

- You see someone removing classified material from the work area without appropriate authorization.
- You observe a colleague using an unclassified fax or computer to transmit classified material.
- You observe a person improperly removing the classification markings from documents.
- You hear a colleague discussing classified information on a nonsecure telephone.
- You become aware that people with TS/SCI or contractors with a reporting requirement have attempted to conceal any work-related foreign travel and any personal foreign travel.

Mail Distribution and Security Concerns

US Classified Confidential mail can arrive at USDA through normal first class mail channels. One way to recognize it is the requirement to have stamped on the outside "POSTMASTER, Do Not Forward."

US Classified Secret mail is sent through Registered Mail or by one of nine approved overnight Express Mail Services.

Here are some tips for you to consider:

- If your office handles classified information and a document arrives that requires a signature, it is best to lock it up in a security container until the recipient of the package is in the office.
- The staff person who receives mail may need to have a Secret security clearance.
- Do not leave mail out overnight – secure it in an area with no public access.
- Do not have the office mailboxes close to a hallway, in a hallway, or other areas with public access.
- Know who your Information Security Coordinator is or whom to call if you receive a classified package by mistake, it is classified but not double wrapped, or it arrived damaged.

The Answers to Your E-QIP Questions

In June, OPM released the "e-QIP Help Desk Manual" to offer solutions to common applicant problems. The manual can be accessed via the OPM Secure Portal under the *OPM Library* link or by contacting the Personnel Security Branch at 202/720-7373.

The manual addresses problems with accessing the system, logging in, filling out the online form, finalizing the completion of your form, and follow-up attempts. It includes actual screen shots from e-QIP to walk you through the solutions, making the guide very user-friendly.

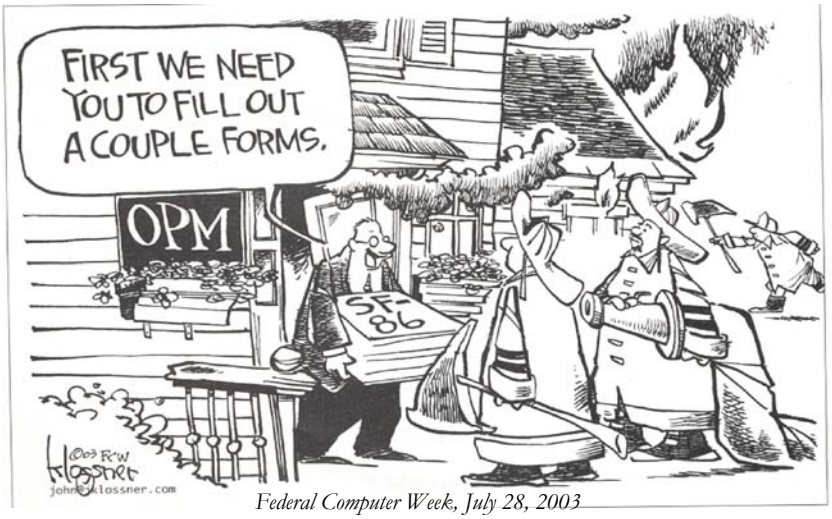
This manual will be helpful to all security points-of-contact as they begin tasking their employees to complete their security questionnaires via e-QIP. This will guide you in answering their questions to common user problems.

WHO'S YOUR INFORMATION SECURITY COORDINATOR?

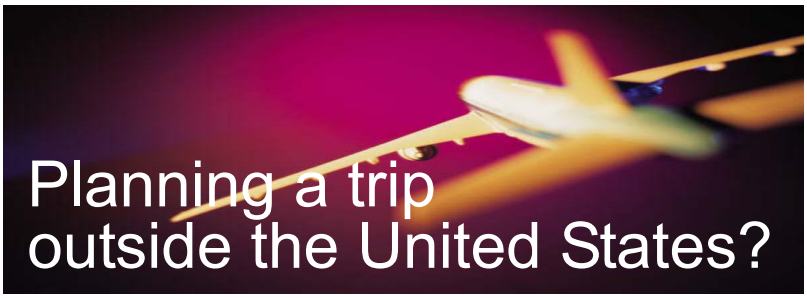
Many USDA Mission Areas and Offices have trained Information Security Coordinators. They can be of assistance if you need to know how to mark and store a classified document properly, coordinate security container combination changes, and who to contact for other questions or problems related to Information Security. If you do not see a person identified who can assist you, please call the Information Security Staff at 202-720-7373 for assistance.

Here are the current coordinators:

Breed, Darrel	Ag Marketing Service	202-690-3045
Cochran, Thomas	Forest Service, Aviation	404-909-1738
Cohen, Ken	OGC	202-720-5565
Crumb, Clarice	FSA, Mgmt Svcs Div	202-690-1560
Eickholt, Brad	Exec Secretariat	202-720-9301
Hooper, Ron	FS, Ofc of Reg & Mgmt Svcs	202-205-1524
Lopez, Wanda	OIG	202-720-4612
Mackall, Andrea	FSIS	202-720-1890
Manis, Mack J.	GIPSA, Safety & Issuance	202-720-0244
Morgan, Rita	Forest Service - Primary	703-605-4910
O'Connor, Michael	Ofc of Operations	202-720-8846
Pollard, Steve	REE,ARS, CSREES, NASS, NAL, ERS	202-720-3359
Quinn, Larry	Ofc of Communications	202-720-4623
Randolph, Sharon	RD, Opers & Mgmt	202-692-0207
Rhodes, Steve	Foreign Ag Service	202-720-1759
Rowe, Carol	NRCS - Primary	202-690-2008
Sheaver, Michael	NRCS - Alternate	301-504-2242
Simoneaux, John	Nat'l Finance Center	504-426-0232
Watson, Cato L.	Food Nutrition Svcs	703-305-2242
Wortman, Darryl	APHIS	301-436-3158



Federal Computer Week, July 28, 2003



Whether you are traveling on business or pleasure, all employees are urged to visit the State Department's travel website (http://travel.state.gov/) for the latest travel warnings, consular information sheets, and trip registration. Registration at the U.S. Embassy or Consulate (in the country you are visiting) makes your presence and whereabouts known, in case it is necessary for a consular officer to contact you in an emergency. During a disaster overseas, American consular officers can assist in evacuation were that to become necessary.

To view the latest travel warnings, click here https://travelregistration.state.gov/ibrs/home.asp.

To register your trip, click here https://travelregistration.state.gov/ibrs/home.asp.

All holders of a security clearance must keep their security office informed about anything that might have a bearing on their continued eligibility for access to classified information or that might signal an increased vulnerability to foreign intelligence targeting. Your cooperation in doing so is an important part of the "continuing evaluation" process.

You are *required* to report all foreign travel if you have been approved for access to Sensitive Compartmented Information (SCI). Please contact Carrie Moore, Senior Personnel Security Specialist, PDSD, via email about your travel plans with two weeks advance notice, if possible.

Following your trip, report any unusual incidents that occurred during your travel to PDSD (202/720-7373).

Insider Espionage Threat is Growing

Opportunities and motivations for espionage by cleared "insiders" are steadily increasing, according to a new study performed for the Department of Defense. There are numerous reasons why the perceived insider threat is growing, the study says.

- Insiders have an unprecedented level of access to classified and proprietary information due to technological advances in information storage and retrieval.
- American employees have greater opportunity to establish contact with foreign entities and to transfer information to them through traveling internationally more often and by participating in international research and business ventures more frequently.
- Internet use is expanding globally and computer-users are becoming more culturally and linguistically diverse. The Internet can now be used to transmit massive amounts of digitized information to multiple foreign parties simultaneously.
- The market for U.S. information is expanding.

Complicating matters further, even the most effective personnel security program will never fully eliminate the insider espionage threat. The DoD study, published in May, is somewhat old-fashioned in the sense that it focuses on information security in isolation and as an independent variable. It does not consider whether there is such a thing as an "acceptable" level of espionage risk, nor does it address the possible adverse consequences of tightening information security controls.

For further information, see "Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage," by Lisa A. Kramer, Richards J. Heuer Jr., and by Kent S. Crawford, Defense Personnel Research Center (PERSEREC), May 2005.

Final Thought…

This is an internal newsletter for USDA employees and contractors. If you would like to see PDSD address a particular topic, process, or guideline in a future newsletter, please submit your request to PDSD at pdsd@usda.gov.

Our Address
1400 Independence Ave, SW
STOP 9305, RMS310
Washington, DC 20250

Phone:
(202) 720-7373

Fax:
(202) 720-7708

E-Mail:
pdsd@usda.gov